Appendix U, DCSOPS-SECURITY CHECKLIST to 1A Cir 1-201

UNIT EVALUATED ______________________________________ **DATE EVALUATED** __________________

INSPECTOR ____ **PHONE:** _______________________

OVERALL RATING: **MET STANDARDS** **NEEDS IMPROVEMENT**

1. PUBLICATIONS. Does the unit have the following references on hand or on requisition?

a. AR 381-12 “Subversion and Espionage Directed Against U.S. Army (SAEDA)” YES NO NA

b. AR 380-67 “Personnel Security Program” YES NO NA

c. AR 380-5 with FORSCOM Suppl “Department of Army Information Security Program” YES NO NA

d. AR 380-19 “Information Systems Security” YES NO NA

2. ADMINISTRATION.

a. Has a properly cleared officer, WO, NCO (E7 or above) or civilian (GS-7 or above) been appointed in writing as security manager? (AR 380-5, para 13-304) YES NO NA

b. Has security manager received training in duties and responsibilities? (AR 380-5, para 13-304) YES NO NA

c. Does security manager have a proper security clearance to the appropriate level required? (original DA Form 873, security clearance) (AR 380-5, para 13-304) YES NO NA

d. Is a FORSCOM Form 102R "your Security manager is" posted in a conspicuous location? (FORSCOM Supplement 380-5, para 5-202) YES NO NA

3. PERSONNEL SECURITY

a. Is security manager aware of procedures for submitting requests for security clearances? (Personnel Security Update 96-4, DCSINT MSG 261225Z Sep 96) YES NO NA

b. Is there a record of: YES NO NA

Initial security briefings (AR 380-5, para 10-102) YES NO NA

Annual Refresher Briefings (AR 380-5, para 10-103) YES NO NA

Foreign Travel Briefings (AR 380-5, para 10-104 with YES NO NA

FORSCOM Suppl and AR 380-67 with FORSCOM Suppl, para 9-203)

Termination Briefings (AR 380-5, para 10-105) YES NO NA

c. Do all members of the unit receive a biennial SAEDA briefing? (AR 381-12, para 6) YES NO NA

d. Does unit maintain a data base on SAEDA briefings for reporting purposes, as to: (AR 381-12, para 5)

Number of personnel in the command? YES NO NA

Number of personnel briefed? YES NO NA

Total number of briefings? YES NO NA

e. Is there a method to insure that absentees and new members received a biennial SAEDA briefing? (AR 381-12, para 6) YES NO NA

f. Does the unit security manager have a copy of the SAEDA briefing? YES NO NA

g. Is there a record of spot checks being made periodically by the security manager to insure compliance with security directives? (FORSCOM Supplement to AR 380-5, para 13-304) YES NO NA

h. Has the security manager determined that assigned personnel are cleared for the security level for which they require access? (AR 380-67, para 7-100a) YES NO NA

i. Does the security manager understand the procedures to obtain verification of a previous clearance; procedures to obtain an initial security clearance; and how to upgrade a security clearance? (AR 380-67, Chapter V) YES NO NA

j. Are the commanders and their appropriate staff members promptly providing adverse information to the security manager? Is adverse information concerning all personnel reported to the security manager regardless of rank or branch of service of the individual? (AR 380-67, Chapter 8 & 9) YES NO NA

k. Does the security manager know what actions are to be taken when derogatory information is reported on an individual with a security clearance? (AR 380-67, Chapter 9, Section 1) YES NO NA

l. Does the security manager maintain a listing (access roster) of personnel authorized access to classified information? Are they properly distributed? (AR 380-5, para 7-200; DAMI-CIS MSG 022000Z Nov 89, Subject: Personnel Security Message 08-89) YES NO NA

m. l. Does the record document (access roster) include the following data? (Para 7-200 and DAMI-CIS MSG 022000Z Nov 89, Subject: Personnel Security Message 08-89) YES NO NA

Name
Rank
SSN
Status; I.E., RC CIV, AGR, AC
Level of Access
Date of Last Investigation

n. Is access roster current? (AR 380-5, para 13-304) Have names of personnel who have left the unit been removed from access roster? (AR 380-5, para 13-304) YES NO NA

o. Does security manager understand the requirement for completing the SF 312 (replaces SF 189) Nondisclosure Agreement? (AR 380-5, para 10-102 & 10-105) YES NO NA

p. Have civilian positions been designated sensitive, and is a record on file officially designating these positions? (AR 380-67, para 3-100 & 3-101) YES NO NA

q. Are SF 189/312 on file for personnel listed on current access roster? (AR 380-5, para 10-102) YES NO NA

r. Does security manager understand The disposition and routing of the second original copy of SF 312? YES NO NA

4. INFORMATION SECURITY

a. Does the security manager understand the procedure for requesting and receiving Courier Authorization cards (DD Form 2501)? (AR 380-5, para 8-300) YES NO NA

b. Is there a record of issue? Has courier been briefed and is there a record of briefing? (AR 380-5, para 10-102) YES NO NA

c. Do copy machines have FORSCOM Poster p-93, Prohibition Notice, posted on each machine not authorized for reproduction of classified? (FORSCOM Supplement to AR 380-5, para 7-305) YES NO NA

d. Is FORSCOM form 138-R posted on or neAR copiers that are used to reproduce classified documents? (FORSCOM Suppl to AR 380-5, para 5-102) YES NO NA

e. Are classified documents stored in a GSA approved container? (AR 380-5, para 5-102) YES NO NA

f. Is the field safe secured to A permanent part of facility? (AR 380-5, para 5-102) YES NO NA

g. Is field safe secured with a 3/8” chain? (AR 380-5, para 5-102) YES NO NA

h. Is chain secured with GSA approved combination or padlock? (AR 380-5, para 5-102) YES NO NA

i. Can security container be opened by person not authorized access? (FORSCOM Supplement to AR 380-5, para 5-104) YES NO NA

j. Are security checks made at the close of each duty day to ensure classified containers are properly locked and SF 702 properly executed? (AR 380-5, para 5-202) YES NO NA

k. Have the rules of classification been properly observed? (AR 380-5, Chapter I, Sections 4, 5, and 6; Chapter II, Sections 1, 2, 3, and 4). Is document marked with “Derived From” line if originated by First U.S. Army unit? YES NO NA

l. Have proper downgrading/declassification markings been applied to documents and messages prepared by the activity? (AR 380-5, Chapter IV, Section 4) YES NO NA

m. Has the custodian automatically downgraded or declassified documents IAW assigned markings? (AR 380-5, Chapter IV, Section 4) YES NO NA

n. Is each section, part, paragraph, or similAR portion of a classified document marked to show the level of classification of the information contained therein, or that it is unclassified? (AR 380-5, para 4-202) YES NO NA

o. Are the front and back covers and title pages (if any) and the first pages of classified documents marked with overall security classification of the document? (AR 380-5, para 4-200) YES NO NA

p. Are tops and bottom of pages of classified documents containing classified information marked with the highest classification of information containing no classified information marked "unclassified"? (AR 380-5, para 4-200) YES NO NA

q. Are subjects and titles of classified documents marked with the appropriate symbol "(U)", "(C)", "(S)", or "(TS)" immediately following and to the right of the item? (AR 380-5, para 2-204) YES NO NA

r. Are SF 702 and SF 700 affixed to classified containers (AR 380-5, para 5-104) YES NO NA

s. Is an up-to-date, properly classified record (SF 700, Part 2 and 2a) of all safe combinations, together with other information necessary to identify and locate the containers, maintained within a control office? Is the envelope appropriately marked? (AR 380-5, para 5-104) YES NO NA

t. Are combinations changed at intervals not exceeding 12 months or upon loss/compromise of combination, change of personnel knowing the combination, or receipt of new containers? (AR 380-5, para 5-104) YES NO NA

u. Does unit properly maintain unused security container, if any? (AR 380-5, para 5-104) YES NO NA

v. Is there a unit plan for Emergency Removal and/or Safeguarding of Classified Material posted in a conspicuous location neAR the security container? (AR 380-5, para 5-203) YES NO NA

w. Are tops of security containers kept free of extraneous materials? (FORSCOM Supplement 380-5, para 5-202) YES NO NA

x. Was annual clean out of unneeded classified materials conducted? (FORSCOM Supplement to AR 380-5, para 9-105) YES NO NA

y. Is the security container free of cash and other high-value item? (AR 380-5, para 5-100) YES NO NA

z. Do personnel know the action to be taken in the event a classified container is found open and unattended, or when it is reported that classified information may be lost or compromised? (AR 380-5, para 6-102) YES NO NA

aa. Are personnel preparing classified documents for transmission outside of the headquarters familiAR with the enveloping, addressing, marking and receipting requirements? (AR 380-5, Chapter 8, Section 2) YES NO NA

bb. Is DA Form 3964 used to transmit secret documents between activities when U.S. Postal Service resources or mail room are used? (AR 380-5, para 8-202) YES NO NA

cc. Is carbon paper used in conjunction with the typing of classified material destroyed as classified waste? (AR 380-5, para 9-104) YES NO NA

dd. Do properly cleared officials witness the destruction of TOP SECRET and accountable SECRET material? Do destruction documents reflect date, identity, and signatures of custodian/top secret control officer and disinterested witness? (AR 380-5, para 9-104) YES NO NA

ee. Are all alterations on DA Form 3964 (Destruction Certificates) initialed by the witnessing official? (AR 380-5, para 9-102) YES NO NA

ff. Is classified waste properly handled and destroyed? (AR 380-5, para 9-104) YES NO NA

gg. Are class 1 shredders (1/32 inch strips w/cross cut) used to destroy TOP SECRET classified documents? (AR 380-5, para K-4b(2)). Is the "Secure Volume" destruction procedure used when destroying classified documents? (AR 380-5, Appendix K) YES NO NA

hh. Is OCONUS travel being reported as required? (AR 380-5, and AR 380-67) YES NO NA

ii. Are official visits by foreign nationals concurred by the activity commander and approved by the office of the Deputy Chief of Staff for Intelligence, Department of the Army? (AR 380-10) YES NO NA

5. INFORMATION SYSTEMS SECURITY

a. Has an information system security officer (ISSO) been appointed for each AIS or group of AIS? (AR 380-19, para 1-6d(3)) YES NO NA

b. Is the ISSO familiAR with his/her responsibilities? (AR 380-19, para 1-6d(3) (a-m)) YES NO NA

c. If applicable, has a network security officer (NSO) been appointed for each network? (AR 380-19, para 1-6d(4)) YES NO NA

d. Is the NSO familiAR with his/her responsibilities? (AR 380-19, para 1-6d(4)(a-i)) YES NO NA

e. Has the AISSM/ISSO attended the Information System Security course (SSC) or equivalent? (AR 380-19, para 2-15) YES NO NA

f. Does the ISSO have knowledge of computer commands and operations? (AR 380-19, para 1-6d(2b)) YES NO NA

g. Does the ISSO have a listing of all NSOs for contact purposes? (AR 380-19, Para 1-6) YES NO NA

h. Has the NSO/ISSO attended the ISSC or equivalent? (AR 380-19, para 2-15) YES NO NA

i. Does the NSO/ISSO have experience with and/or have knowledge of computer commands and operations? (AR 380-19, para 1-6d) YES NO NA

j. Is the current version of anti-virus software installed (no more than one version older than current version)? (AR 380-19, para 2-27) YES NO NA

k. Have procedures been established to report suspected or actual virus infections to AISSM/ISSO, and reporting to the ISSM? (AR 380-19, para 2-27) YES NO NA

6. ISS ACCREDITATION/REACCREDITATION:

a. Are all AIS accredited? (AR 380-19, para 3-1) YES NO NA

b. Are all accreditations current? (AR 380-19, para 3-6) YES NO NA

c. Does the AIS have the correct sensitivity designation? (AR 380-19, para 2-2a(1-2)) YES NO NA

d. Has the AIS been designated with the correct mode of operation? (AR 380-19, para 2-2b(1-4) YES NO NA

e. Are any employee-owned AIS required to be approved for use IAW AR 25-1 and in compliance with, including accredited, AR-380-19? (AR 380-19, para 2-24a) YES NO NA

f. Do AIS have appropriate classification labels affixed? (AR 380-19, para 2-19) YES NO NA

g. Have unclassified warning labels "This Equipment Will Not Be Used to Process “Classified Material” been posted to all PCs? (AR 380-19, para 2-19) YES NO NA

h. Is there a “Classification label for notebook/laptop computers? (AR 380-19, para 2-19) YES NO NA

i. Is a log-on banner notice included as part of the log-in screen on all computer system? (AR 380-19, para 4-1l) YES NO NA

j. Are classified diskettes, ribbons, etc., properly marked when unclassified data is processed in the same general area as classified? (AR 380-19, para 2-19) YES NO NA

k. Are all classified materials (i.e., diskettes, ribbons, etc.) marked and stored IAW appropriate guidelines/regulations? (AR 380-19, para 2-19) YES NO NA

l. Is classified information that is being processed on system with non-removable hard drives being properly protected? Is the system in an area approved for open storage? Is the system stored in a GSA approved security container? (AR 380-19, para 2-21) YES NO NA

m. Is all classified information transmitted only by secure means? (AR 380-19, para 4-2) YES NO NA

n. Is unclassified-sensitive information protected in transmission by NSA approved techniques or has a waiver been approved for the transmission? Is waiver on file? (AR 380-19, para 4-3 (b&c)) YES NO NA

o. Are privately owned computers being used to process government data at the unit/activity? (This response should be a negative. If affirmative, answer “P” below.) (AR 380-19, para 2-25) YES NO NA

p. Is an approval letter from DOIM to use privately owned computers on file? (AR 380-19, para 2-24) YES NO NA

7. ISS ACCESS AND ACCOUNTABILITY:

a. Except for “small computers” is there an audit trail employed that will ensure all users of the AIS may be held responsible for their actions? (AR 380-19, para 2-3a(1)) YES NO NA

b. Are all proposed changes to the AIS configuration, (i.e., software, hardware, facility or environmental), reported to the ISSO for determination of the security implication of the change? (AR 380-19, para 2-12c(3)) YES NO NA

c. Is software properly accounted for and stored? (AR 380-19, para 2-4) YES NO NA

d. Is the activity in compliance with commercial/proprietary copyright/licensing agreements (i.e., one licensed copy of software per system or the command has a site license)? (AR 380-19, para 2-4) YES NO NA

e. Are master copies of all proprietary software protected from unauthorized use, abuse, or duplication? (AR 380-19, para 2-4) YES NO NA

f. Is property accounted for and stored properly? (AR 380-19, para 2-14c(4)) YES NO NA

g. Is access system utilized on the AIS? (AR 380-19, para 2-3a(2)) YES NO NA

h. Does the ISSO generate and issue all passwords? (AR 380-19, para 2-14b) YES NO NA

i. Are users aware of the prohibition of disclosing their password to other personnel? (AR 380-19, para 2-14d) YES NO NA

j. Are passwords randomly generated for AIS processing SCI/SIOP-ESI with a minimum of five character strings using the 36 alphabetic-numeric characters or six character string using only alphabetic characters? (AR 380-19, para 2-14i) YES NO NA

k. Are non-US citizens utilized to perform maintenance on AIS designated as CS3 and below? (AR 380-19, para 2-9c) YES NO NA

l. Do all for authorized access to AIS have an initiated or favorably completed PSI which at least meets the scope of an ENTNAC or NAC? (AR 380-19, para 2-16) YES NO NA

8. PHYSICAL CONTROLS:

a. Is the AIS locked in an office or otherwise secured to prevent loss or damage when all users leave the AIS Area? (AR 380-19, para 2-11) YES NO NA

b. Are any maintenance personnel cleared to the highest level which the AIS is accredited to process or are they observed during maintenance by individuals with the technical background to detect obvious unauthorized modifications? (AR 380-19, para 2-9b) YES NO NA

c. Is an approved security software package being used? (AR 380-19, para 2-4d & 2-6a) YES NO NA

d. Is the security software the same as that described and evaluated in the risk management program? (AR 380-19, para 2-6b) YES NO NA

e. Are passwords inhibited, overprinted or otherwise protected from unauthorized observation on terminals and video displays? (AR 380-19, para 2-14h) YES NO NA

f. Is there a current listing of specifically developed or approved software authorized for use by the U.S. Government that identifies approved software for use on the specific AIS? (AR 380-19, para 2-4b&d) YES NO NA

g. Is there a master copy of the authorized software maintained and not used for actual operations production? (AR 380-19, para 2-4f) YES NO NA

h. Are all users required to log off the AIS when they leave the area? (AR 380-19, para 2-11c(3)) YES NO NA

i. Are only approved cryptosystems being used for encryption of transmitted classified information? (AR 380-19, para 4-1c(1-3)) YES NO NA

j. Has a contingency plan been developed? (AR 380-19, para 2-3a(11)) YES NO NA

k. Are system and application program libraries protected and backup copies maintained? (AR 380-19, para 2-4f) YES NO NA

9. ISS SECURITY TRAINING:

a. Does the unit have a "security training and awareness" program for all personnel involved in the operations of AIS? (AR 380-19, para 2-15) YES NO NA

b. Is an initial security briefing, which covers the minimum requirements prescribed in AR 380-19, para 2-15a (1-8), provided to all users? YES NO NA

c. Are periodic security briefings, covering the minimum requirements prescribed in AR 380-19, para 2-15b(1-5), provided to all security managers and users? YES NO NA

10. ISS SECURITY PLANNING AND RISK MANAGEMENT:

a. Is the unit AIS SOP security plan readily available for all managers or users as a reference? (AR 380-19, para 3-2e(4)) YES NO NA

b. Has a review been conducted to identify any changes in the operating environment described by the accreditation package that require the updating or appending of the SOP and security plan? (AR 380-19, para 5-6) YES NO NA

c. Does the security plan address utilization of employee owned AIS? (AR 380-19, para 2-24)	YES	NO	NA
d. Does the AIS SOP and security plan prohibit the use of employee-owned AIS for processing classified national defense information? (AR 380-19, para 2-24a)	YES	NO	NA
e. Does the AIS SOP and security plan address utilization of laptop or portable AIS? (AR 380-19, para 2-26)	YES	NO	NA
f. Are any laptop AIS with nonremovable hard drives that process classified material, stored in an approved storage area when left unattended? (AR 380-19, para 2-26c)	YES	NO	NA
g. Does the AIS SOP address in sufficient detail the procedures to be followed in the event of discovering an AIS security incident? (AR 380-19, para 2-27 & App C-8)	YES	NO	NA
h. Does the security plan of networked systems address encryption for those transmitting US1, Unclassified-Sensitive Information, as well as, Classified National Defense Information, CS3, CS2, or CS1? (AR 380-19, para 4-3b)	YES	NO	NA
i. Does the ISSM maintain a central accreditation inventory with the date of AIS accreditations/reaccreditations, sensitivity levels, security mode of operation, organization, equipment make, model, and serial number? (AR 380-19, para 1-6d(1))	YES	NO	NA

11. SECURITY OF SUPPLIES AND EQUIPMENT

a. Is there a system to control, account for, and secure administrative keys, to include vehicle keys? (AR 190-51, App D, para d)	YES	NO	NA
b. Is a key custodian appointed to issue and receive keys and maintain accountability for office, unit or activity keys? (AR 190-51, App D, para d-2)	YES	NO	NA
c. Is the key control register kept in a locked container with controlled access? (AR 190-51, App D, d-3)	YES	NO	NA
d. Is a key access roster published? (AR 190-51, App D, para d-7)	YES	NO	NA
e. Are keys issued with signature on authorized key control register? (AR 190-51, App D, d-3)	YES	NO	NA
f. Does key depository meet minimum security standards? (AR 190-51, App D, para d-4)	YES	NO	NA
g. Are keys properly secured? (AR 190-51, App D, para d-6)	YES	NO	NA

h. Are exterior doors secured with adequate locking devices? (AR 190-51, Apps B and D) YES NO NA

i. Are Level I or higher security measures met if required for any items? (AR 190-51, Chap 3, Section II and FR III) YES NO NA

j. Are outside areas used for vehicle storage enclosed by security fencing and protected by security lighting, if required? (AR 190-51, para 3-5) YES NO NA

k. Are local law enforcement agencies requested in writing to check the security of motor pool areas during non-operational hours? (AR 190-51, para 3-5f(1)(b)) YES NO NA

l. Is a semiannual inventory of keys and padlocks conducted? (AR 190-51, App D, para d-6) YES NO NA

m. Are keys issued by the key custodian, alternate, or designated individual? (AR 190-51, App C, para c-1) YES NO NA

n. Are hand tools, tool sets and kits, and shop equipment properly secured and controlled? (AR 190-51, para 3-22) YES NO NA

o. Are night vision devices adequately secured? (AR 190-51, para 3-6) YES NO NA

12. ANTI-TERRORISM/FORCE PROTECTION

a. Has operational responsibility been established for Force Protection for all units and individuals whether permanently or temporarily assigned? (AR 525-13, para 4-3) YES NO NA

b. Has Anti-Terrorism/Force Protection training been implemented and documented to include viewing of AT/FP videos and issuance of the Individual Protective Measures tri-fold card (GTA 21-3-11) and A Self-Help Handbook to Combating Terrorism, JS Guide 5260? If an individual is traveling to a medium or high threat area, has an additional briefing been conducted by a certified Level II AT/FP instructor? (AR 525-13, para 4-17) YES NO NA

c. Has a Combating Terrorism/Force Protection plan been developed which details appropriate protective and preventive measures during periods of a heightened threat IAW AR 525-13? (AR 525-13, para 4-4 and 4-7) YES NO NA

d. Are written procedures established for disseminating time sensitive threat information during duty and non-duty hours to all personnel? (AR 525-13, para 4-16) YES NO NA

e. Has an FP awareness program been developed and incorporated into the Command Information Program? (AR 525-13, para 4-13) YES NO NA

f. Have individuals identified as having significant FP responsibilities received training IAW their duties? (AR 525-13, para 4-18) YES NO NA

COMMENTS:____